# CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

Directive Current as of 18 December 2014

J-3 CJCSI 3209.01
DISTRIBUTION: A, B, C 9 January 2012

DEFENSE CRITICAL INFRASTRUCTURE PROGRAM

References: See Enclosure D

1. Purpose. This instruction assigns duties and responsibilities for the Defense Critical Infrastructure Program (DCIP).

2. Cancellation. None.

3. Applicability

a. This instruction applies to the Joint Staff, the Military Departments, combatant commands, Defense agencies, DOD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DOD Components").

b. This instruction provides guidance to the Defense Infrastructure Sector Lead Agents (DISLAs), which are identified in reference a.

4. Policy

a. The Department of Homeland Security's National Infrastructure Protection Plan is the U.S. government program to identify and protect critical infrastructure/key resources (CI/KR), systems, and assets so vital that their loss may have a debilitating impact on the security, economy, public health or safety, and environment from the local to national level of the United States. These assets are primarily civilian owned/operated. The Department of Defense does not have a direct role in the protection, remediation, or mitigation of CI/KR assets beyond those it owns.

b. DCIP is the DOD risk management program that seeks to ensure the availability of Defense Critical Infrastructure (DCI) and identify Task Critical

Assets (TCAs) necessary to support the National Military Strategy. The DCIP process leads to risk management decisions by responsible authorities to ensure the capability to execute those mission essential functions. DCIP complements the efforts of, but is not subordinate to, DOD programs that contribute to mission assurance through risk management such as: Antiterrorism, Readiness, Information Assurance (IA), Continuity of Operations (COOP), Chemical, Biological, Radiological, and Nuclear Consequence Management (CBRN CM), and Installation Emergency Management.

c. Asset owners bear the responsibility to manage risk to the infrastructure they own in coordination with appropriate mission owners.

d. The Chairman of the Joint Chiefs of Staff shall advise, coordinate, integrate, assess, and report on the development of DCIP processes, procedures, and implementation.

e. The Office of the Secretary of Defense, in coordination with the Joint Staff, will implement and coordinate the risk management process for Defense Critical Assets (DCAs). For each DCA, the asset owner will develop a Risk Decision Package (RDP) with at least two risk reduction courses of action from which senior leadership can select remediation options. RDPs will be coordinated with the appropriate DOD Components, to include all mission owners.

5. Definitions. See Glossary.

6. Responsibilities

a. The Joint Staff. See Enclosure A.

b. Combatant Commanders. See Enclosure B.

c. Chiefs of the Military Departments. See Enclosure C.

d. Commander, U.S. Special Operations Command. In addition to Enclosure B tasks for combatant commands, carry out those Enclosure C responsibilities appropriate to the command's Service-like roles.

e. Chief, National Guard Bureau. Support DCIP through vulnerability assessment teams.

f. Sectors and DISLAs

(1) Provide DCIP support to DOD Components.

(2) Sectors with TCAs supporting their Sector Functions will coordinate with the appropriate DOD Service or agency that owns the TCA to conduct appropriate DCIP responsibilities.

7. Summary of Changes. None.

8. Releasability. This instruction is approved for public release. Distribution is unlimited. DOD components, other federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--http://www.dtic.mil/cjcs_directives. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

9. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

WILLIAM E. GORTNEY
VADM, USN
Director, Joint Staff

Enclosures:

A – THE JOINT STAFF
B – COMBATANT COMMANDS
C – SECRETARIES OF THE MILITARY DEPARTMENTS
D – REFERENCES
GL - GLOSSARY

(INTENTIONALLY BLANK)

# ENCLOSURE A

## JOINT STAFF

1. The Chairman will appoint a Joint Staff Office of Primary Responsibility (OPR) for the DCIP. The OPR is the Chairman's principal DCIP coordinator and is responsible to build and maintain a network of functional experts from the Joint Staff Directorates and the other DOD Components to collaborate and cooperate on DCIP issues. Additionally, the OPR is the lead Joint Staff representative to the Defense Critical Infrastructure Integration Staff (DCIIS). The Joint Staff must maintain a long-term, strategic view of the DCIP effort while maintaining an awareness of all DCIP operational activities on the Joint Staff. In addition to coordinating with combatant commands and Military Departments, Joint Staff directorates must coordinate as required with the DCIP Sectors and DISLAs.

2. The J-1 will:

a. Advise the Chairman and the DCIP OPR on all DCIP personnel related issues.

b. Support the J-5 review of the DCIP section of all Combatant Commanders' operational and contingency plans.

c. Support and coordinate with the Personnel DISLA.

3. The J-2 will:

a. Advise the Chairman and the DCIP OPR on all DCIP intelligence-related issues.

b. Serve as the Joint Staff lead for all intelligence issues related to DCIP.

c. Support the J-5 review of the DCIP section of all Combatant Commanders' operational and contingency plans.

d. Support and coordinate with the Intelligence and Space DISLAs and the interagency as required.

4. The J-3 will:

a. Execute the duties of the DCIP OPR.

b. Advise the CJCS on all DCIP operational related issues and the Global Information Grid (GIG).

c. Facilitate the Joint Staff Defense Critical Infrastructure Program Implementation Plan; with the J-5 coordinate DCIP policy and guidance; coordinate with OASD (HD&ASA).

d. Represent the Joint Staff on DCIP operational issues; support the J-5 in interagency policy forums.

e. Support the J-5 review of the DCIP section of all Combatant Commanders' operational and contingency plans.

f. Facilitate coordination among DOD Components on DCIP issues and related programs and strategies, to include, but not limited to: Physical Security, Antiterrorism, Force Protection, COOP, CBRN CM, Installation Emergency Management, IA, and Readiness activities and programs.

g. Lead Joint Staff participation at DCIP formal conferences to include the DCIIS; convene/chair the DCIP Business Rules Working Group as required.

h. Coordinate DCIP assessments:

(1) Oversee the DCIP assessment program in concert with OASD (HD&ASA).

(2) Develop and oversee a scheduling process and the execution of DCIP related assessments.

(3) Ensure DCAs are assessed at a minimum triennially; in order to support development of a complete risk picture, multiple assets that function as a system, or that support a common mission, will be assessed together; those assets that are geographically separated yet function as a system may be assessed separately, but must still meet the triennial requirement.

(4) OPR will review Combatant Commands' DCIP program as part of the triennial Higher Headquarters Assessment.

i. Ensure organizations conducting DCIP vulnerability assessments provide subject matter experts (SME) as team members; utilize DCIP standards and benchmarks.

j. Evaluate asset owner and mission owner DCA recommendations and forward final CJCS nominations to ASD(HD&ASA) for approval.

k. Serve as the focal point for consolidating assessment data; support the development and direct the use of appropriate coordination tools to support DCIP scheduling and information sharing utilizing platforms that have a secure, ".mil" address.

l. Ensure DOD Components monitor and report DCIP-related data on threats, hazards, vulnerabilities, and related trends; assist the Undersecretary of Defense for Intelligence, OASD(HD&ASA), and J-2 in implementing processes for monitoring, reporting, and sharing DCIP-related information.

m. Ensure the mitigation action(s) selected by responsible authorities are implemented. Coordinate with DOD Components, the DISLAs, and with other government agencies and non-governmental DCI owners and operators with which DOD relies.

n. Provide DCIP information in support of Defense Support of Civil Authorities (DSCA)/consequence management operations and exercises.

o. Support and coordinate with the GIG DISLA; provide advice on and support to the globally-interconnected, end-to-end set of information capabilities and associated processes.

p. Co-lead the Data Exchange Working Group.

q. Serve as the Joint Staff lead for cyber-related DCIP issues (J39) in collaboration with the OPR (J34).

r. Coordinate, communicate, and participate with DOD Components and DISLAs on DCIP related IA and Computer Network Operations issues.

s. Attempt to resolve DCI coordination issues between mission and asset owners (such as Baseline Elements of Information (BEI), mitigation efforts, or RDPs. If unable to resolve, JS DCIP OPR will forward unresolved issues to OASD(HD&ASA) for resolution.

5. The J-4 will:

a. Advise the Chairman and the DCIP OPR on all DCIP logistics and Defense Industrial Base (DIB)-related issues.

b. Coordinate, communicate, and participate with the Combatant commands, the Military Services, and DISLAs to assist in the integration of all logistics functions with DOD DCIP efforts.

c. Support the J-5 review of the DCIP section of all Combatant Commanders' operational and contingency plans.

d. Support and coordinate with the Health Affairs, Transportation, Logistics, and Public Works DISLAs.

e. Inform the DCIP OPR regarding logistics implications for interagency national critical infrastructure and DIB related issues.

6. The J-5 will:

a. Advise the Chairman, the DCIP OPR, and J-4 on interagency national critical infrastructure, DCIP Information Assurance policy related issues, and DIB related issues and DCIP policy matters and DCIP conventional war plan issues.

b. Represent the Joint Staff at national level CIP policy forums such as the Homeland Security Council and associated working groups and with other departments/agencies chartered with coordination of CIP policy issues.

c. With the DCIP OPR, support OASD(HD&ASA) to develop and coordinate strategic DCIP policy.

d. Coordinate the review of DCIP-related sections of all Combatant Commanders' operational and contingency plans. Identify DCIP-related resource deficiencies with potential impact to Operation Plans (OPLANs) and include these deficiencies when appropriate in the Joint Force Readiness Review (JFRR). Consider these deficiencies when validating DCIP priorities for the Integrated Priority List (IPL).

e. Support and coordinate with the DIB DISLA, OASD(HD&ASA), and the interagency as required.

f. Serve as the Joint Staff Protected Critical Infrastructure Information Program lead.

g. Coordinate with the Defense-wide IA Program and other IA-specific advisory groups to integrate IA into the DCIP.

7. The J-7 will:

a. Advise the Chairman and the DCIP OPR on all DCIP-related Joint Force Development issues.

b. Advise and assist DCIP SMEs who wish to develop or change DCIP doctrine IAW reference o.

c. Advise and assist DCIP SMEs who wish to integrate DCIP into Force Development processes.

d. Support the J-5 review of the DCIP section of all Combatant Commanders' operational and contingency plans.

8. The J-8 will:

a. Advise the Chairman on all DCIP resource and funding related issues.

b. Inform the DCIP OPR regarding Joint Staff DCIP resource, budget efforts, and an annual summary of DCIP expenditures.

c. Coordinate, validate, and advocate DCIP funding, resource requirements, and remediation efforts for the combatant commands in line with Joint Capability Areas.

d. Conduct strategic analysis and assessment of DOD's DCIP requirements as directed by the Joint Requirements Oversight Council.

e. Support the J-5 review of the DCIP section of all Combatant Commanders' operational and contingency plans.

f. Lead coordination efforts of the Joint Staff to develop and incorporate policy requirements for assessment and management of risk to existing and new critical assets/systems/infrastructure to minimize or eliminate current or future DCIP TCAs.

g. Support and coordinate with the Financial Services DISLA.

9. The Comptroller will:

a. Advise the Chairman and the DCIP OPR on all DCIP resource and funding related issues.

b. Support J-8 to develop and incorporate policy requirements for assessing risk management of new assets/systems/infrastructure to minimize or eliminate future DCIP TCAs. Support funding for emerging DCIP requirements.

(INTENTIONALLY BLANK)

# ENCLOSURE B

## COMBATANT COMMANDERS

1. Combatant Commanders will:

a. Execute DCIP responsibilities per references a through f.

b. Establish a command DCIP Program.

(1) Establish a DCIP OPR; resource and execute a command program for identification and prioritization of DCI. Establish or leverage existing coordination processes with Service Components (or applicable Service POCs) to address DCIP requirements.

(2) Verify Service Components coordinate with their Service for all required mission capabilities provided by the parent Military Department.

(3) IAW references c and f, conduct mission decomposition, review and validate TCAs submitted by DOD Components; assign tier levels to TCAs based on Combatant Command mission impact and use of the Critical Asset Identification Process (CAIP).

(4) Coordinate with asset owners to update BEI when new TCAs are identified or changes occur. Additionally, combatant commands/mission owners will coordinate with DISLAs when sector specific assets are identified. Relate TCA BEI data to numbered plans.

(5) Ensure mission owners provide input to asset owners during the coordination phase of RDP development.

(6) Submit to the Joint Staff DCIP OPR changes to command DCIP requirements, including priorities for DCIP assessment and risk mitigation responses to DCI-related assessed risks.

(7) Maintain awareness of the execution of DCIP Vulnerability and Risk Assessments and Risk Management within the respective Service component commands.

(8) Include DCI in joint exercises, education, outreach, and training activities.

(9) Prepare Appendix 16 (DCIP) to Annex C (Operations), Joint

Operation Planning and Execution System (JOPES) Volume II for each OPLAN: Appendix 16 will describe and address how infrastructure failure or degradation would affect capabilities necessary to execute the OPLAN. Ensure planning addresses required DCIP actions to ensure the availability of DOD and non-DOD cyber and physical infrastructure networks critical for mission success.

(10) Include identified DCIP readiness deficiencies in the JFRR per reference p. A Readiness Deficiency is a shortfall of resources to meet the requirements of a reporting organization's assigned mission, plan, or other documented responsibility. Consider this information when setting DCIP priorities for the IPL.

b. In coordination with the DOD asset owner, the heads of other DOD components, and DISLAs, act to manage the risk to critical assets against all likely threats and hazards within the assigned AOR. Act to prevent or mitigate the loss or degradation of non-DOD owned critical assets only at the direction of the Secretary of Defense, with the exception of immediate response to prevent significant damage to mission-critical infrastructure.

c. Establish reporting mechanisms for asset owners to report on the operational status, threats, and hazards to Defense Critical Infrastructure. Forward reports to the Joint Staff DCIP OPR, as appropriate.

d. Submit a report detailing the status of DCIP Milestones as required. Combatant commands will forward reports to the Joint Staff DCIP OPR.

# ENCLOSURE C

## SECRETARIES OF THE MILITARY DEPARTMENTS AND COMMANDER, U.S. SPECIAL OPERATIONS COMMAND

1. Per DOD policy, Secretaries of the Military Departments and the Services will:

a. Per reference b, establish and maintain a DCIP program supporting DOD DCIP requirements. Report program implementation status and resourcing data as required.

b. Establish or leverage existing coordination processes between DOD Components to ensure the identification of missions, functions, tasks, standards, and conditions required to complete mission decomposition successfully.

c. IAW references c and f, ensure BEI data is complete and coordinate with mission owners to ensure critical infrastructure is tiered appropriately. Identify how degradation/failure of critical infrastructure impacts planning efforts and assigned missions.

d. Asset owners will assess all Tier 1 TCAs; develop courses of action to address identified vulnerabilities/threats/hazards or other concerns for prioritization by responsible authorities.

e. Coordinate and oversee the execution of DCIP Assessments; submit to the Joint Staff DCIP OPR and other appropriate offices changes to command DCIP requirements, including priorities for DCIP vulnerability assessments and submission of RDPs.

f. Recommend assets as DCAs to OSD and the Joint Staff DCIP OPR IAW the CAIP or when asset status changes. Ensure RDPs are developed and submitted for DCAs as required by DCIP policy. Provide mission owners the opportunity to review RDPs during the coordination phase of RDP development. Submit recommendations to downgrade asset criticality when changes occur to missions, mission impact, or the creation of redundant assets and alternate capabilities.

g. Incorporate DCIP in Service planning, exercises, education, and training programs. Training and exercises should inform and test the roles of individuals at all levels, to include installations of their role relating to DCI. Installations and organizations need to understand both the concept and the identity of their DCI. Execute annual exercises, either separately or in conjunction with existing exercises, to integrate other federal departments and

agencies in the risk reduction and in the protection, recovery, and restoration of assets affected by the full spectrum of threats and hazards.

h. Provide DCIP information in support of DSCA/consequence management operations and exercises.

# ENCLOSURE D

# REFERENCES

a. DOD Directive 3020.40, 14 January 2010, "Defense Critical Infrastructure Program"

b. DOD Instruction 3020.45, 21 April 2008, "Defense Critical Infrastructure Program (DCIP) Management"

c. DOD Manual 3020.45 V1, 24 October 2008, "Defense Critical Infrastructure Program (DCIP): DOD Mission-Based Critical Asset Identification Process (CAIP)"

d. DOD Manual 3020.45 V2, 28 October 2008, "Defense Critical Infrastructure Program (DCIP): DCIP Remediation Planning"

e. DOD Manual 3020.45 V4, 20 March 2009, "Defense Critical Infrastructure Program (DCIP): Defense Critical Asset (DCA) Nomination and Submission Process"

f. DOD Manual 3020.45 V5, 24 May 2010, "Defense Critical Infrastructure Program (DCIP): Execution Timeline"

g. DOD Directive 5100.01, 21 December 2010, "Functions of the Department of Defense and Its Major Components"

h. JSM 5100.01 series, "Organization and Functions of the Joint Staff"

i. The Joint Staff Deputy Directorate for Antiterrorism and Homeland Defense, June 2009, "Defense Critical Infrastructure Program Implementation Plan"

j. Homeland Security Presidential Directive 7 (HSPD-7), 17 December 2003, "Directive on Critical Infrastructure Identification, Prioritization and Protection"

k. The White House, May 2010, "The National Security Strategy of the United States of America"

l. Office of Homeland Security, July 2002, "National Strategy for Homeland Security"

m. Office of Homeland Security, February 2003, "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets"

n. "Department of Defense Mission Essential Functions (MEFs) (U)," Volume 2

o. CJCSI 5120.02 series, "Joint Doctrine Development System"

p. CJCSI 3401.01 series, "Joint Combat Capability Assessment"

# GLOSSARY

## PART I - ACRONYMS

| | |
|---|---|
| ASD | Assistant Secretary of Defense |
| ASD (HD&ASA) | Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs) |
| BEI | Baseline Element of Information |
| CAIP | Critical Asset Identification Process |
| CCIF | Combatant Commander's Initiative Fund |
| DCA | Defense Critical Asset |
| DCI | Defense Critical Infrastructure |
| DCIIS | Defense Critical Infrastructure Integration Staff |
| DCIP | Defense Critical Infrastructure Program |
| DEWG | Data Exchange Working Group |
| DISLA | Defense Infrastructure Sector Lead Agent |
| GIG | Global Information Grid |
| IA | Information Assurance |
| IPL | Integrated Priority List |
| JFRR | Joint Force Readiness Review |
| JSIVA | Joint Staff Integrated Vulnerability Assessment |
| MAD | Mission Assurance Division |
| MEF | Mission Essential Function |
| OASD | Office of the Assistant Secretary of Defense |
| OPR | Office of Primary Responsibility |
| RDP | Risk Decision Package |
| SMADS | Strategic Mission Assurance Database System |
| TCA | Task Critical Asset |
| USACE | United States Army Corps of Engineers |

## PART II – DEFINITIONS

Unless otherwise stated, the terms and definitions contained in this glossary are for the purposes of this instruction only.

Continuity: Uninterrupted connection, union, duration or continuation, especially without essential change.

Defense Critical Infrastructure Integration Staff: A cooperative partnership assisting the OASD (HD&ASA) DCIP Directorate with planning, coordinating, integrating and administering DCIP-related programs. Also called DCIIS.

DCIP Assessment: A comprehensive assessment of a Defense Critical Asset consisting of an in-depth look based on current DOD DCIP Assessment benchmarks.

Interagency: Of or pertaining to United States Government agencies and departments, including the Department of Defense.